ON THE GENERALIZATION AND EXTENSION OF SYLOW'S THEOREM.

By PROFESSOR G. A. MILLER, Stanford University.

Cauchy proved that every prime number which divides the order of a group (G) is itself the order of at least one subgroup of G. Let p represent any prime which divides the order of G and suppose that α has been so chosen that p^α is the highest power of p which is the order of a subgroup of G. Such a subgroup may be denoted by P_α, and we may suppose that P_α contains only one subgroup (P_β) of order p^β and of a particular type. This condition is always fulfilled when $\beta=\alpha$, but, in many cases, it may also be satisfied for smaller values of $\beta>0$.

We proceed to prove that the number of the subgroups in G which are of the same type as P_β is of the form $1+kp$. If one of these subgroups would transform another into itself the two would generate a group ($P_{\beta'}$) of order $p^{\beta'}$, $\beta'>\beta$. Hence the number of the subgroups of order p^α is of the form $1+kp$, and every operator of order p^γ which transforms one of these subgroups into itself must be in this subgroup. Since no subgroup of order p^δ could transform each one of the $1+kp$ subgroups of order p^α into another, it follows that every subgroup of order p^δ is found in $1+mp$ subgroups of order p^α.* In particular, $P_{\beta'}$ must be contained in a subgroup of order p^α. This is impossible if all the subgroups of order p^α are conjugate since P_β contains at least two subgroups of the same type as P_β while P_α contains only one such subgroup.

That the $1+kp$ subgroups of order p^α form a single conjugate set may be seen as follows: If they did not form a single set, they could be divided into more than one set such that each set would include only those which are conjugate under G. Since P_α (or any subgroup of P_α which is not contained in another group of order p^α) transforms each of the other subgroups of order p^α into a different one, it follows that the set which includes P_α must include $1+k'p$ subgroups while each other set must include a multiple of p subgroups. Since P_α is any of the subgroups of order p^α this result is impossible. Hence all the subgroups of order p^α form a single conjugate set and the number of the subgroups of order p^β which are of the same type as P_β is of the form $1+kp$. The latter constitute a single conjugate set since the subgroups of order p^α form a single congugate set.

Since p^α is the order of a subgroup of G it must divide the order of G. That no higher power of p divides this order follows from the fact that the order is $p^\alpha h(1+kp)$, where $p^\alpha h$ is the order of the largest subgroup of G which transforms P_α into itself. If h were divisible by p, G would contain a subgroup of order $p^{\alpha+1}$ Hence we have the results:

*Several of the arguments of this proof depend upon the fact that any group of order p^n transforms operators and subgroups in sets of p^β, where β may be 0.

(1) *The number of subgroups which are of the same type as* P_β *is of the form* $1+kp$.

(2) *All of these subgroups form a single conjugate set.*

(3) *The order of* G *is of the form* $p^\beta h_1(1+kp)$, *where* $p^\beta h_1$ *is the order of the largest subgroup of* G *which transforms* P_β *into itself.*

By letting $\beta=\alpha$ in these results we have Sylow's theorem. When $\beta=\alpha$ the factor h_1 is not divisible by p, while it is divisible by p for all other values of β.

If G is represented as a substitution group it is only necessary that P_α does not contain two similar subgroups of order p^β. It may be observed that characteristic subgroups of P_α may be conjugate under G. For instance, in the simple group of order 168 all the subgroups of order 2 are conjugate while the subgroups of order 8 contain a characteristic subgroup of order 2. If P_α contains just m sets of conjugate subgroups of a given order, G cannot contain a larger number of such sets but it may contain a smaller number. In particular, all the subgroups of order p^α in G are conjugate since P_α contains only one subgroup of this order.

The preceding relates to generalizations of Sylow's theorem. The main extension of this fundamental theorem is due to Frobenius and affirms that the number of subgroups of order p^δ, $\delta \overline{\gtrless} \alpha$, is of the form $1+kp$, but that these subgroups do not necessarily form a single set of conjugates except when $\delta=\alpha$. It is clear that every subgroup of order p^δ which is transformed into itself by P_α must be contained in P_α. Hence P_α transforms all the subgroups of order p^δ which are not contained in it in sets each containing p^ϵ ($\epsilon>0$) subgroups. That is, if the number of subgroups of order p^δ in P_α is of the form $1+kp$, the number of those in G must be of the same form.

It remains to prove that the number of invariant subgroups of order p^δ in P_α is of the form $1+kp$. Let P_δ represent any one of these invariant subgroups. All the others have some largest subgroup in common with P_δ. The common subgroup is clearly invariant under P_α. We proceed to prove that the number of those subgroups of order p^δ (excluding P_δ) which have a particular subgroup in common with P_δ is always a multiple of p. If the common invariant subgroup is not the identity, the number of these is equal to the number of subgroups (less one) of a certain order in the corresponding quotient group. As the theorem may be supposed true for for all groups whose order is less than p^α it may be assumed true for each one of these quotient groups. That is, the number of invariant subgroups of order p which have a particular subgroup (not the identity) in common with P_δ and are different from P_δ is a multiple of p.

It remains only to consider the case when the largest common subgroup is the identity. In this case P_α contains one or more direct products of P_δ and some other group of order p^δ. In such a direct product $[P_\delta, P_\delta']$ all the subgroups of order p^δ which have only the identity in common with P_δ can be obtained by establishing a β, 1 isomorphism between P_δ' and some subgroup of P_δ. Moreover, all the groups which can be constructed in this manner are in this direct product. For any particular subgroup of P_δ whose order exceeds p the number

of such isomorphisms is a multiple of p, since the order of the group of isomorphisms of any group of order p^γ ($\gamma>0$) is divisible by p. Hence there are always a multiple of p such subgroups for every possible value of $\beta<p^{\delta-1}$.

When $\beta=p^\delta$ there is clearly only one group, viz, P_δ'. When $\beta=p^{\delta-1}$ there are $p-1$ such groups for every subgroup of order $p^{\delta-1}$ in P_δ' and any particular subgroup of order p in P_δ. Since $\delta<\alpha$, we may assume that the required theorem is true with respect to P_δ and P_δ'. Hence the number of the required subgroups for $\beta=p^{\delta-1}$ and p^δ is of the form $(n_1p+1)(n_2p+1)(p-1)+1$. That is, the number of subgroups of order p^δ which have only identity in common with P_δ and are contained in the direct product $[P_\delta, P_\delta']$ is also a multiple of p. All of these subgroups are simply isomorphic with P_δ'. This completes the proof that P_α contains just $1+kp$ subgroups of order p^δ.

In some cases it is easy to extend this extension of Sylow's theorem. For instance, we may readily see that the number of subgroups of order $p^{\alpha-1}$ in P_α is of the form $\dfrac{p^m-1}{p-1}$.* To see this interesting fact we may observe that any subgroup of order $p^{\alpha-1}$ has just $p^{\alpha-2}$ operators in common with any other subgroup of this order. These common operators form an invariant subgroup of P_α, which includes its commutator subgroup since the corresponding quotient group is abelian. It also includes the pth power of every operator of P_α since this quotient group is of type (1, 1). Hence the operators which are common to all the subgroups of order $p^{\alpha-1}$ form an invariant subgroup including the pth power of every operator of P_α as well as its commutator subgroup. The corresponding quotient group is therefore abelian and of the type (1, 1, 1, ...). Since the subgroups of order p^{m-1} in this quotient group correspond to groups of order $p^{\alpha-1}$ in P_α and since the former number is equal to the number of sub-groups of order p in the quotient group of order p^m, the theorem is proved.

Another interesting extension is the fact that the number of subgroups of order p in P_α is of the form $1+p+kp^2$ whenever there is more than one such subgroup and p is odd. This extension is clearly included in the following theorem:

All the operators of order p in P_α which have not more than p conjugates constitute (with the identity) a subgroup. If all of these operators are invariant the theorem is evident. If this is not the case we may associate a subgroup of order $p^{\alpha-1}$ with each of the non-invariant operators of order p. The common operators of all these subgroups form an invariant subgroup which includes the commutator subgroup of P_α and is composed of the operators which are commutative with each of the operators of the group generated by the given operators of order p. The required theorem follows directly from this property if we bear in mind the well known equations

$$\left.\begin{array}{l} t^{-n}st^n=s_1s \\ (st^{-1})^n=s_1^{[n(n-1)]/2}t^{-n} \end{array}\right\}\text{whenever } s_1 \text{ and } s \text{ are commutative.}$$

A somewhat different way of stating this theorem is as follows: If a

*Bauer, Nouvelles Annales de Mathematiques, 1900, Vol. 19, p. 508.

number of operators of order $p>2$ generate a group under which each one of these operators has no more than p conjugates then the entire group contains no operator whose order exceeds p. It should however be observed that while this condition is sufficient it is by no means necessary to insure the fact that the resulting group contains no operator whose order exceeds p.

It seems well to add that the greater part of this paper aims to present known results in a connected form. The theorem relating to the number of subgroups of order p is, however, supposed to be new and evidently admits of further generalization. The method of proving Frobenius' extension of Sylow's theorem is also supposed to be new.

THE THEORY OF OPTICAL SQUARES.

By PROFESSOR ARNOLD EMCH, The University of Colorado.

1. Optical squares* as they are used in surveying owe their usefulness to the fact that the incident rays from an object include constant angles with the corresponding final reflected rays. The proof for this constancy is a simple application of the geometric proposition that the sum of the angles of any triangle is equal to two right angles.

The ordinary optical square is an entirely special case of a multiple "square" whose geometrical theory and its most important application I propose to present in this paper.

2. This theory results from a close investigation of Poncelet's famous problem: *To construct a rectilinear polygon whose vertices shall lie on given straight lines (one on each) and whose sides shall pass through given points (one through each).*

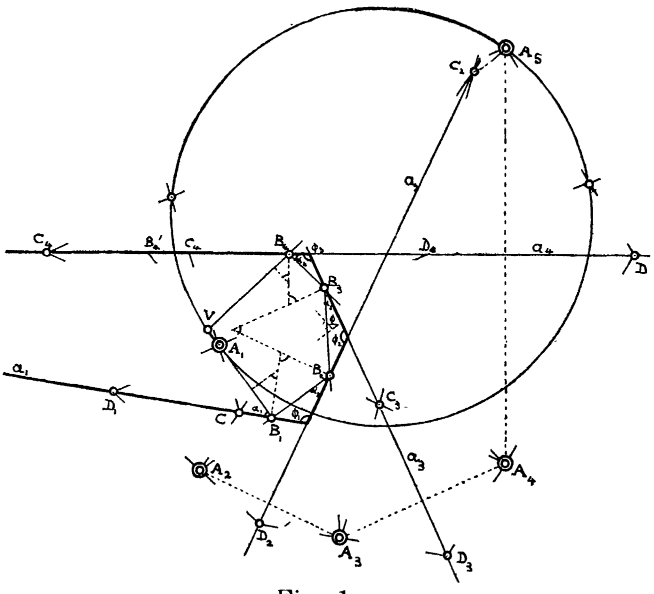

Fig. 1.

*For a description of optical squares (angular mirrors) see G. F. Barker's Physics, Advanced Course, pp. 410-414, or any good text-book on surveying.

†Traite des proprietes projectives des figures (1822), p. 345, or 2nd ed., tome I, p. 281. See also Cremona: Elements of projective geometry, p. 184.